

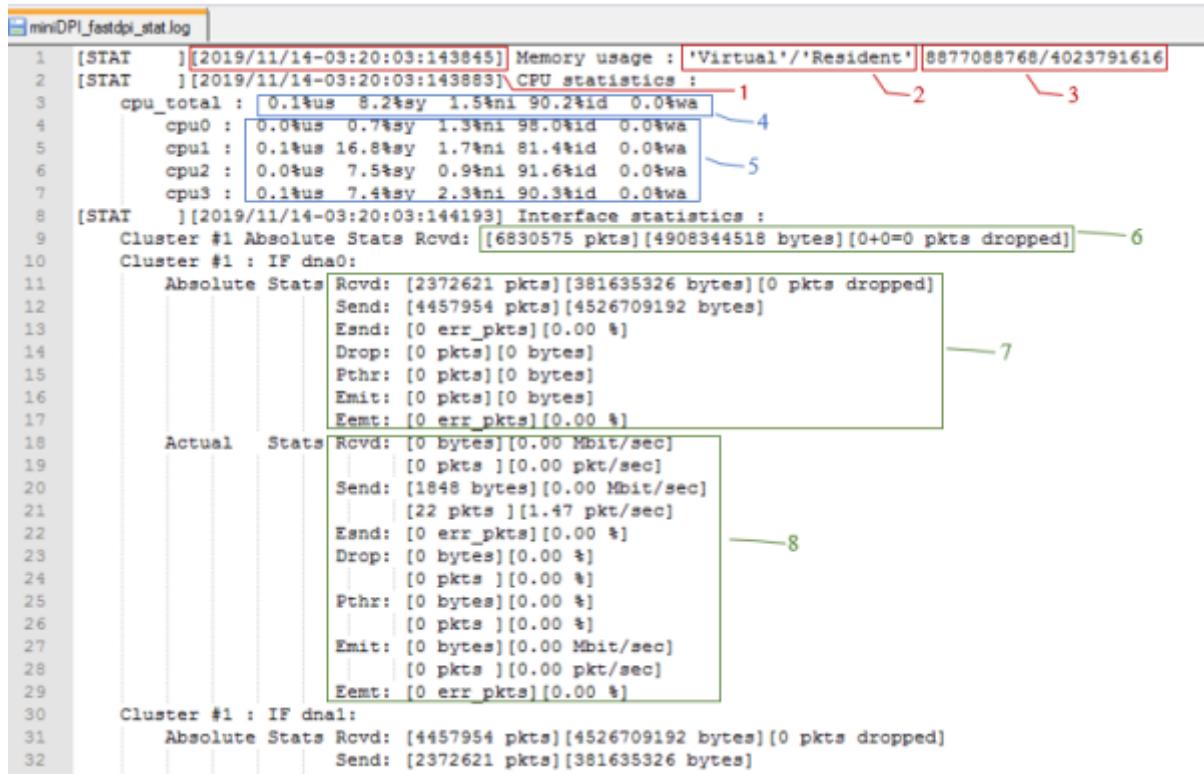
Table of Contents

fastdpi_stat.log	3
-------------------------------	---

fastdpi_stat.log

Находится в папке: `/var/log/dpi/fastdpi_stat.log`

В данном логе хранится статистика по трафику, который обрабатывает СКАТ DPI, что им блокируется, по загруженности памяти, процессора (файл **stat.log**).



Screenshot of the 'miniDPI_fastdpi_stat.log' log file. The log entries are numbered 1 through 32. Red annotations point to specific sections: 1 points to CPU statistics for 'cpu_total', 2 points to the memory usage section, 3 points to the total memory usage value, 4 points to 'cpu0' statistics, 5 points to 'cpu1' statistics, 6 points to the 'Interface statistics' section, 7 points to the 'Absolute Stats' for 'dn0' on line 11, and 8 points to the 'Actual Stats' for 'dn0' on line 18. The log entries show various performance metrics like CPU usage, memory usage, and network interface statistics (Rcvd, Send, Esnd, Drop, Pthr, Emit, Eemt) for different clusters and interfaces.

Рисунок 1

Информация представляется в следующем порядке (см. рис. 1, рис. 2):

- Используемая память:
 - 1 – дата и время съема информации,
 - 2 – тип памяти,
 - 3 – объем.
- Загрузка процессора:
 - 4 – общая загрузка,
 - 5 – загрузка по ядрам.
- Статистика по интерфейсам СКАТ DPI:
 - 6 – полная статистика принятых пакетов/ байт, заблокированных пакетов на всех интерфейсах,
 - 7 - полная статистика принятых пакетов/ байт, заблокированных пакетов на интерфейсе dn0, здесь:
 - Rcvd: [2372621 pkts][381635326 bytes][0 pkts dropped] – принятые пакеты/ байты
 - Send: [4457954 pkts][4526709192 bytes] – переданные пакеты/ байты
 - Esnd: [0 err_pkts][0.00 %] - ошибки, возникшие при отправке пакетов
 - Drop: [0 pkts][0 bytes] – заблокировано пакетов/ байт
 - Pthr: [0 pkts][0 bytes] - количество пакетов/ байт, проходящих без анализа и обработки

- Emit: [0 pkts][0 bytes] - пакеты, которые сформировал СКАТ
- Eemit: [0 err_pkts][0.00 %] - ошибки, возникшие при отправке пакетов, сформированных СКАТ

8 - фактическая статистика принятых пакетов/ байт, заблокированных пакетов на интерфейсе dna0,

9 - совокупная статистика, сколько захвачено, обработано, отправлено пакетов/ сек (см. рис. 2), в примере [Captured 1.47 pkt/sec][Processed 1.47 pkt/sec][Send 0.00 pkt/sec].

IPv4_thread_slave=#1 или 0 - статистика по потоку (0 или 1) - номер потока.

```

0   10   20   30   40   50   60   70   80   90   100  110
31          Absolute Stats Rcvd: [4457954 pkts][4526709192 bytes][0 pkts dropped]
32          Send: [2372621 pkts][381635326 bytes]
33          Esnd: [0 err_pkts][0.00 %]
34          Drop: [0 pkts][0 bytes]
35          Pthrd: [0 pkts][0 bytes]
36          Emit: [0 pkts][0 bytes]
37          Emt: [0 err_pkts][0.00 %]
38          Actual  Stats Rcvd: [1848 bytes][0.00 Mbit/sec]
39          Send: [22 pkts ][1.47 pkt/sec]
40          Esnd: [0 bytes][0.00 Mbit/sec]
41          Drop: [0 pkts ][0.00 pkt/sec]
42          Emt: [0 bytes][0.00 %]
43          Pthrd: [0 bytes][0.00 %]
44          Emit: [0 bytes][0.00 %]
45          Emt: [0 bytes][0.00 Mbit/sec]
46          Drop: [0 pkts ][0.00 pkt/sec]
47          Pthrd: [0 bytes][0.00 %]
48          Emit: [0 bytes][0.00 Mbit/sec]
49          Emt: [0 err_pkts][0.00 %]
50          Cluster #1 : Aggregated Actual stats: [Captured 1.47 pkt/sec][Processed 1.47 pkt/sec][Send 0.00 pkt/sec]
51 [STAT ] [2019/11/14-03:20:03:144266] IPv4_Statistics 'flow nodes' :
52 IPv4_thread_slave#0 : 0/71689/156905/1763/0 ( 986/0/155919 ) ( 0-0/0-0/0-0-0 )
53 0/0/60000/60000 ( 0/0/0/0/0/0 )
54 IPv4_thread_slave#1 : 0/72190/64551/1036/0 ( 722/0/63829 ) ( 0-0/0-0/0-0-0 )
55 0/0/60000/60000 ( 0/0/0/0/0/0 )
56 IPv4_total : allocate=1708/3008000 ( 0/143879/221456/2799/0/7 ) ( 1708/0/219748 ) ( 0-0/0-0/0-0-0 )
57 0/0/120000/120000 ( 0/0/0/0/0/0 )
58 IPv4_actual: new=0 [0 flw/sec] close=0 [0 flw/sec] rei=0 [0 flw/sec]
59 [STAT ] [2019/11/14-03:20:03:144298] IPv4_Statistics 'IP nodes' allocation :
60 total : allocate=5320/6000000
61 [STAT ] [2019/11/14-03:20:03:144308] Detailed statistics on HTTP :
62 thread_slave#0 :
63 url/lock=37475/0 ( 1022,154,0 )( 1,155,154 )
64 ssl/lock=15249/0 ( 0,28,0 )( 1,29,28 )
65 cna/lock=6799/0 ( 0,0 )
66 sni/lock=8450/0 ( 0,28 )
67 quic/lock=0/0 ( 0,0,0 )( 0,0,0 )
68 chnprc=0
69 ccheck/ip_check/lock=372832/45263/0 0/0/0
70 thread_slave#1 :
71 url/lock=40654/0 ( 2069,52,0 )( 1,52,51 )
72 ssl/lock=13571/0 ( 0,6,0 )( 1,7,6 )
73 cna/lock=6081/0 ( 0,0 )
74 sni/lock=7490/0 ( 0,6 )
75 quic/lock=0/0 ( 0,0,0 )( 0,0,0 )
76 chnprc=0
77 ccheck/ip_check/lock=638907/55221/0 0/0/0
78 Total :
79 url/lock=78129/0 ( 3091,206,0 )( 2,207,205,80000 )
80 ssl/lock=28820/0 ( 0,34,0 )( 2,36,34,320000 )
81 cna/lock=12880/0 ( 0,0 )
82 sni/lock=15940/0 ( 0,34 )
83 quic/lock=0/0 ( 0,0,0 )( 0,0,0 )
84 chnprc=0
85 ccheck/ip_check/lock=1011739/100484/0 0/0/0
86 [STAT ] [2019/11/14-03:20:03:144500] FRWL statistics : 0/0/0
87 [STAT ] [2019/11/14-03:20:03:144516] Statistics on NFLW_Full : {765/0/1441180}
88 NFLW_Full IPv4[2316051/888480643]/f4159619/3978665341/{340/1315/1804}
89 [STAT ] [2019/11/14-03:20:16:145013] Memory usage : 'Virtual'/'Resident' 8877088768/4023791616
90 [STAT ] [2019/11/14-03:20:18:145054] CPU statistics :
91 cpu_total : 0.0hus 7.8Msy 0.1hn1 92.0Mhd 0.0hwa
92 cpu0 : 0.0hus 0.3Msy 0.0hn1 99.7Mhd 0.0hwa
93 cpu1 : 0.1hus 16.7Msy 0.3hn1 83.0Mhd 0.0hwa
94 cpu2 : 0.0hus 5.0Msy 0.0hn1 95.0Mhd 0.0hwa
95 cpu3 : 0.1hus 8.7Msy 0.1hn1 91.1Mhd 0.0hwa

```

Рисунок 2

- Статистика по протоколам:

- Статистика по IP:

10 - текущее количество потоков (flow), где

IPv4_total : allocate=1708/3008000 - параметр задается в /etc/dpi/fastdpi.conf: mem_tracking_flow (в примере=3008000)

3008000 - всего / 9055029 – занято

- Счетчики по блокировкам:

url/lock=341/5 (0,0)(1,1,0,98879)

ssl/lock=47/0 (21,457)(0,69,69,196647)

chnprc=0

ccheck/ip_check/lock=2954/503/76

url/lock - проверено url/ заблокировано

- (0,0) :
 - первый 0 - кол-во url, которые не смогли распарсить
 - второй 0 - кол-во пакетов с частичными url (url идет в нескольких пакетах)
- (1,1,0,98879) :
 - 1 - используется парсеров
 - 1 - всего было использовано парсеров
 - 0 - сколько освобождено после использования
 - 98879 - сколько может быть создано
- ssl/lock - аналогично url, только для спама
- chnprc=0 - изменение парсера http ↔ https
- ccheck/ip_check/lock - 2954/503/76 статистика проверки по IP/порт
- 2954 - должны были выполнить проверку по IP
- 503 - сколько раз реально выполнялась проверка
- 76 - заблокировано пакетов

- Статистика по фаерволу - **11**.
- Статистика по netflow - **12**,

```
[STAT      ][2019/02/01-17:21:28:938274] Statistics on NFLW_Full :
{0/0/1668468}
NFLW_Full_IPv4{3948181/939339852}{3111140/3415836963}{7760/13036/6640}
Первые 3 цифры - {0/0/1668468} : { ошибки connect/flow освобождено/нечего
отправлять - счетчики пакетов не изменились }
NFLW_Full_IPv4{3948181/939339852}{3111140/3415836963}{7760/13036/6640} :
{3948181/939339852} : пакеты/байты для direction = 0 ( ip_src < ip_dst )
{3111140/3415836963} : пакеты/байты для direction = 1
{7760/13036/6640} : не отправили по full netflow/ipfix - кол-во flow/пакеты
direction==0/пакеты direction==1
```

Для IPv6 аналогично, но называется NFLW_Full_IPv6

stat --flow

1. IPv4/IPv6
2. всего выделено записей
3. очередь с коротким временем жизни :
 - 3.1 - занято записей
 - 3.2 - готово к повторному использованию
 - 3.3 - разница 3.1 - 3.2 (кол-во активных flow)
4. тоже для долгоиграющей очереди
5. тоже суммарно

stat --proto

1. внутренний индекс статистики по протоколу
2. имя протокола
3. номер порта для протокола

направление subs → inet
4. кол-во пакетов
5. объем в байтах ip total
6. дропнуто пакетов
7. дропнуто байт

направление inet → subs
- кол-во пакетов ит.д.

